Access Control Prefix Router Advertisement Option for IPv6

smb@research.att.com

http://www.research.att.com/~smb

973-360-8656

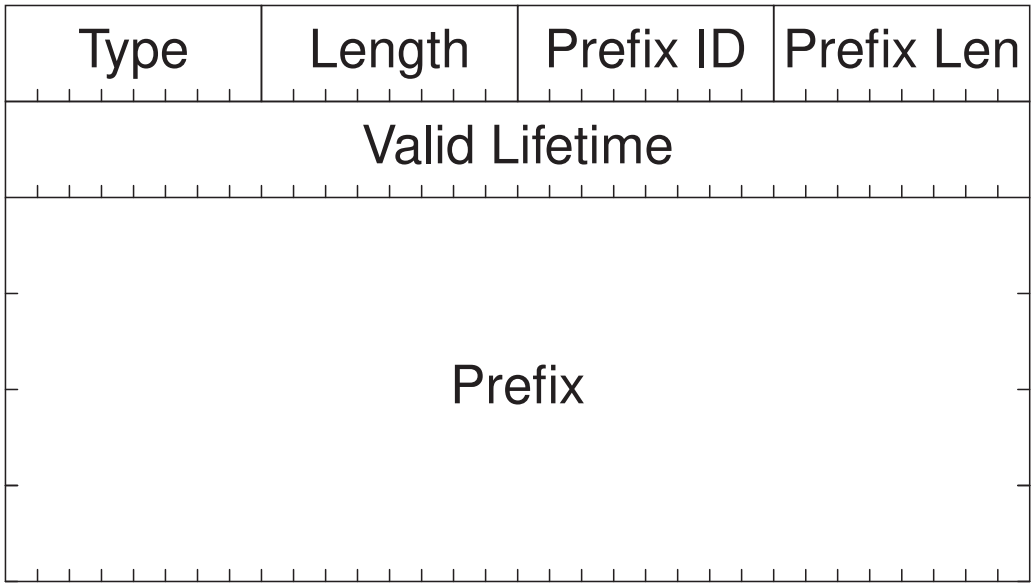
AT&T Labs Research

Florham Park, NJ 07932

Why?

- One of the motivations for site-local addresses is simple access control: how do you control permissions for your IPv6-enabled light bulb?
- An explicit prefix provides more flexibility without the other complexities of site-local.

Option Format



Access control prefixes are identified by Prefix ID, and can be deleted by setting their lifetime to 0.

Node Rules

- Devices MAY be configured to use this option.
- Such devices MUST NOT send packets to other prefixes.
- Packets from other prefixes MUST be dropped.
- Link-local packets and DAD packets MUST be acceptable.
- Access control prefixes are per-interface.

Router Rules

- Routers MAY send this option.
- Multiple access prefixes MAY be announced, but SHOULD be consistent except during deliberate change.
- Routers SHOULD notice and log inconsistencies in announcements from other routers.

This Draft vs. Zill's

- Very similar in intent.
- Zill allocates another flag and field in the Prefix Information option.
- Control is by matching prefix/length, rather than Prefix ID.
- Are there interactions between the option's different uses? (What of a prefix that is on-link with an access option that is longer than the link prefix? What is a preferred lifetime for access control?)
- How does it interact with router renumbering? (How does my draft interact with router renumbering?)

Security Risks

- This is not a strong access control mechanism!
- On-link attackers can forge any prefix.
- On-site attackers can abuse their privileges.
- Etc.